SecureStepPartner

The Tactical Sandbox

Stress-Testing Your Incident Response in a Custom Reality

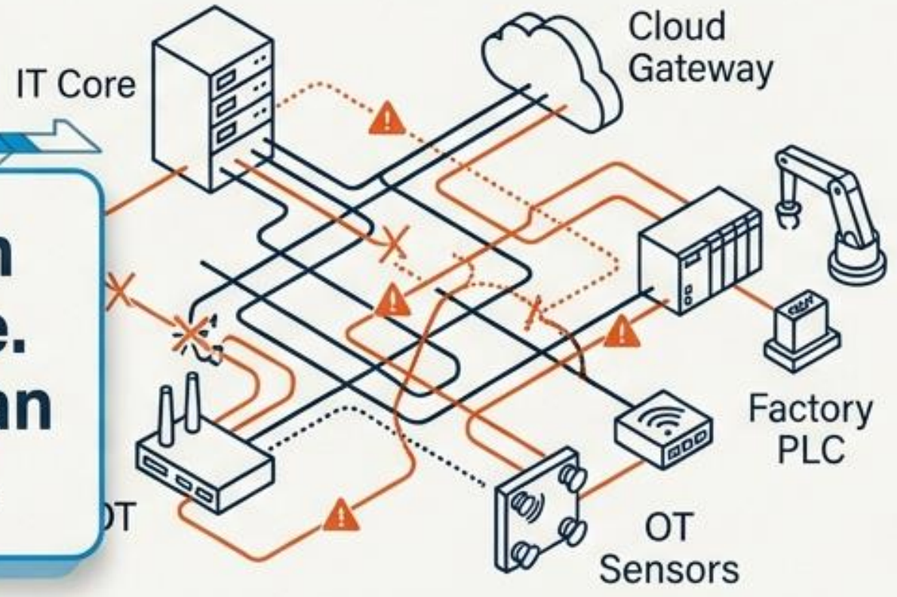
A visual guide to tabletop exercises and the critical gap between having a plan and surviving an attack.

The Illusion of Readiness

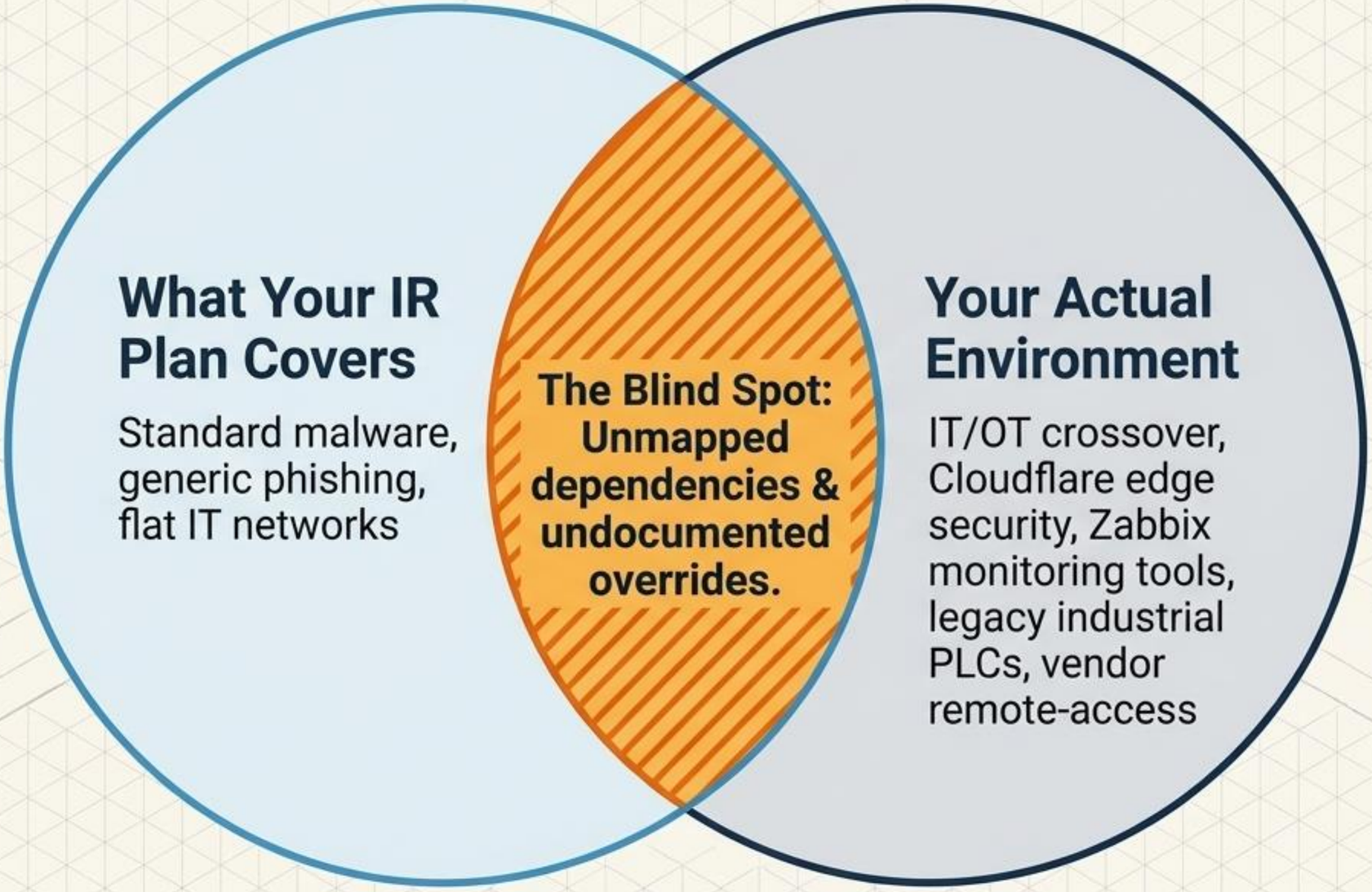
- Assumes flat networks
- Assumes predictable attackers
- Assumes seamless communication

Having a plan is compliance. Testing the plan is resilience.

The Messy Reality



- IT/OT network convergence
- Undocumented legacy systems
- Unavailable executives
- Shifting threat actor tactics



Most organizations don’t fail because they lack tools. They fail because no one owns security across IT, OT, vendors, and cloud when an incident hits.

1. Simulate

Introduce a discussion-based cyber threat scenario.

2. Stress-Test

Apply the scenario directly to your custom architectural constraints and specific business operations.

3. Evaluate

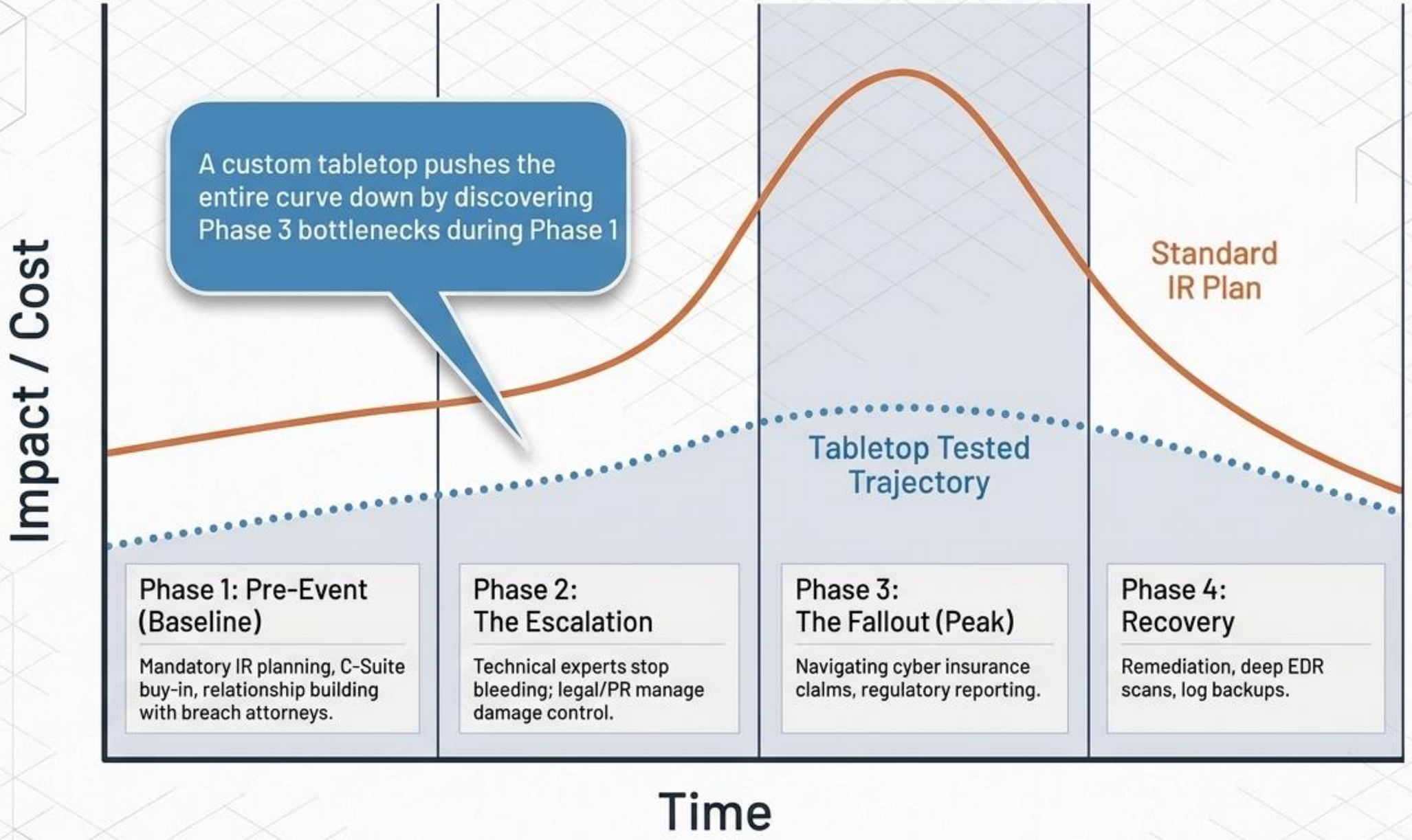
Discover the strengths, weaknesses, and bottlenecks in existing response procedures.

4. Elevate

Update the IR and Business Continuity (BCP) plans with real-world insights.

The Custom Context Imperative

Dimensions	Generic Tabletop	Environment-Specific Tabletop
Threat Vectors	✓ Standard phishing emails	✓ **Targeted** IT/OT crossover attacks and identity abuse
Architecture	✓ Assumed single-tenant cloud	✓ **Your specific hybrid setup** (Huntress MDR, Microsoft 365, local OT assets)
Outcomes	✓ Checking an annual compliance box	✓ **Discovering actual choke points** in your specific tech stack
Engagement	✓ Theoretical discussion	✓ Will our cyber insurance actually cover **THIS specific failure**?



One Incident, Two Fronts

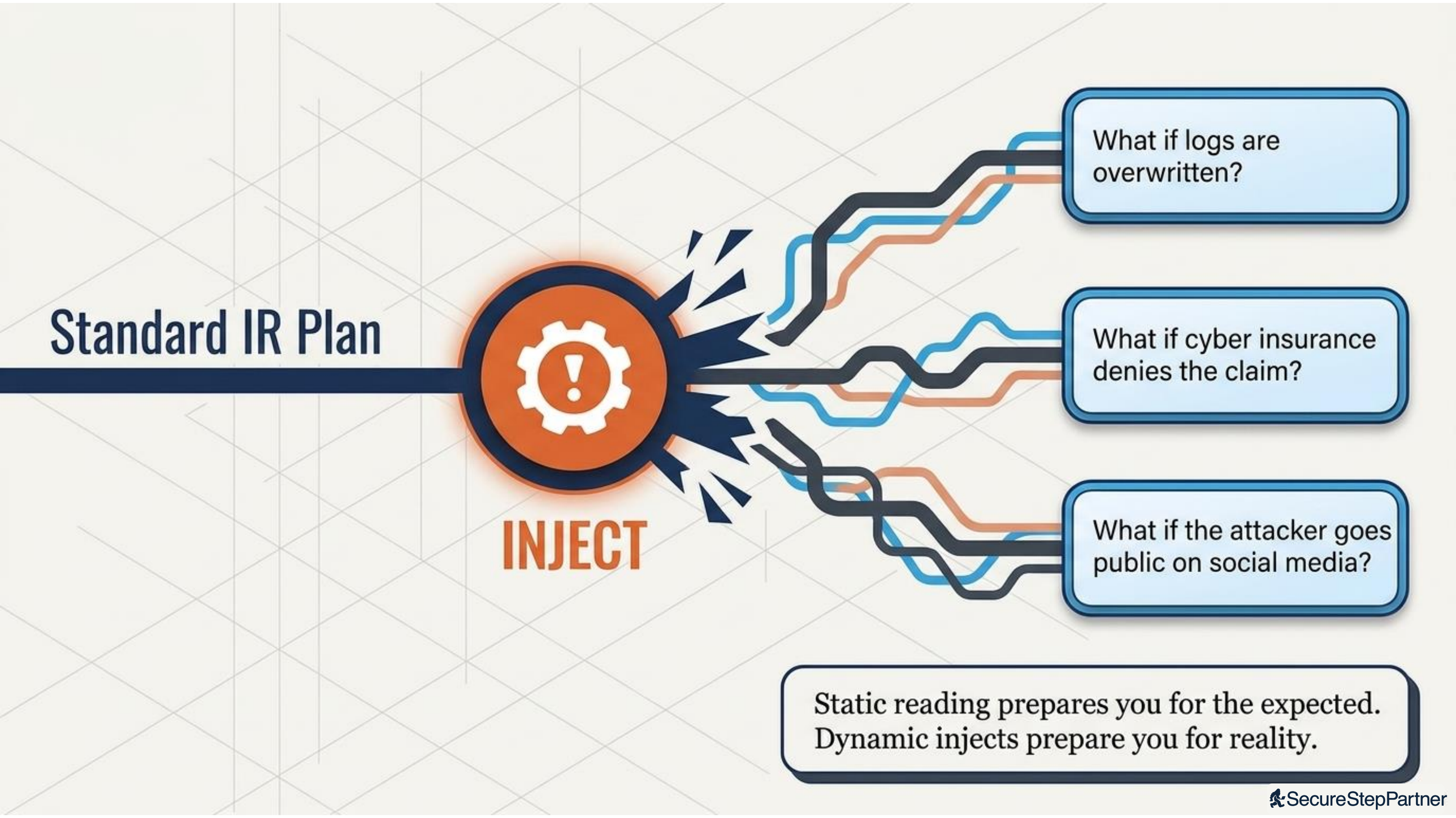
Business Leads

Focus:	Critical decision-making and communications (CEO, COO, Legal).
Tasks:	Attorney/client privilege, PR damage control, insurance negotiation, deciding whether to pay a ransom.

Technical Leads

Focus:	Containment, isolation, and restoration (Sysadmins, Engineers).
Tasks:	Disconnecting affected endpoints to protect memory forensics, patching systems, compiling logs, hunting for persistence.

A tabletop reveals where these two fronts fail to communicate.



Scenario Sandbox: Exposed RDP & Ransomware

The Reality Check: Navigating the Injects

The Insurance Failure

Your cyber insurance **denies** the ransomware claim because **MFA wasn't enabled** (a contract requirement). What's your funding backup?

The Forensics Blackout

Windows Event Logs rolled over due to brute force attempts. Shadow copies are deleted. How do you hunt for persistence now?

The Double Extortion

Attackers **exfiltrated data** during remediation and are demanding a **second ransom** under threat of a public social media leak. Who handles the PR?

Scenario Sandbox: Pwned Identities & Lost Revenue

The Reality Check: Compounding Failures

The Pre-existing Condition

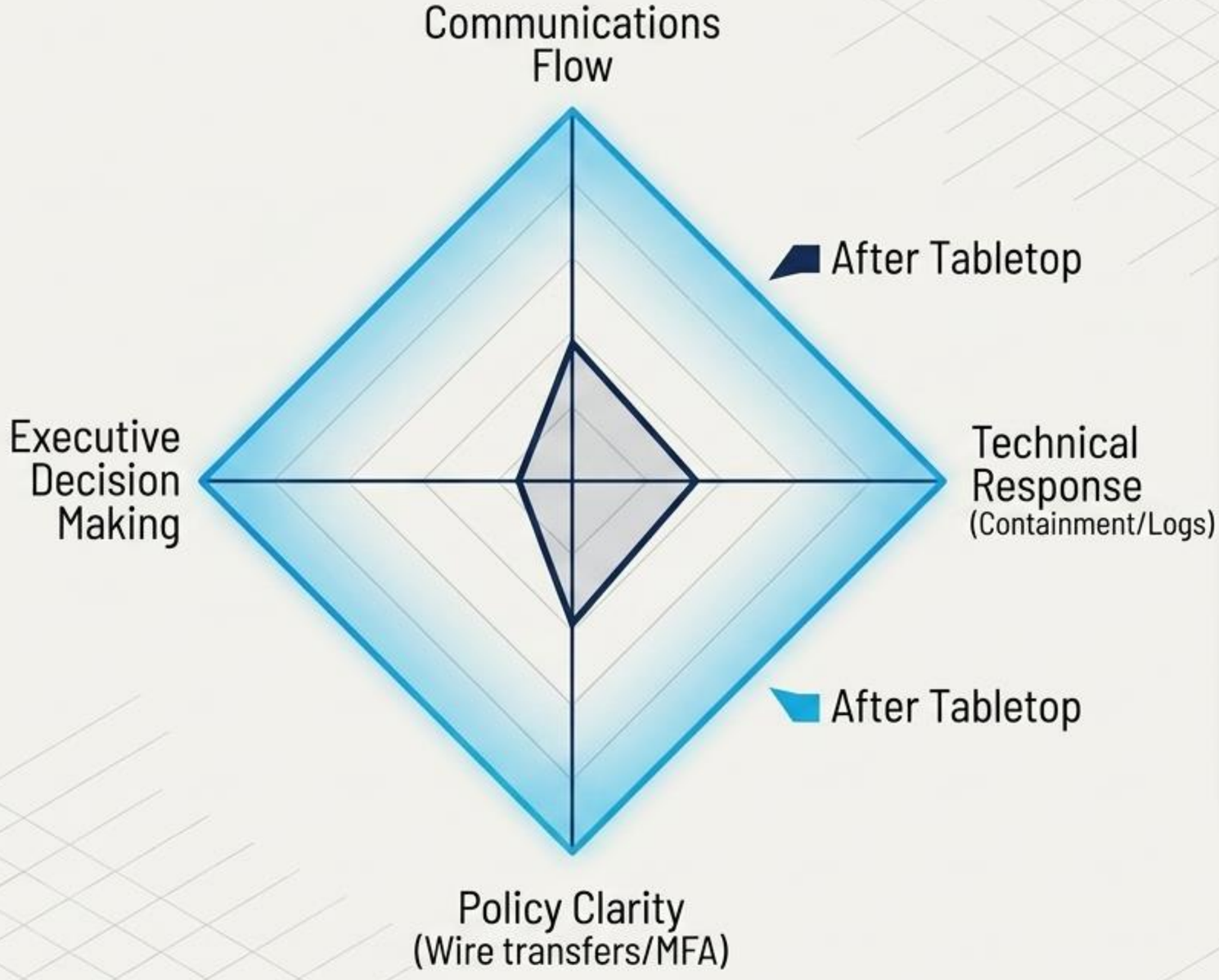
The CFO fell for a similar phishing scam weeks ago. The attacker already has access to multiple high-level accounts.

The Executive Override

The executives didn't like the extra step of MFA, so it was turned off on their accounts. Will insurance cover this?

The Bank Rejection

Due to a delay in recognizing the fraud, the bank refuses to return the $30,000. How does this impact operations?



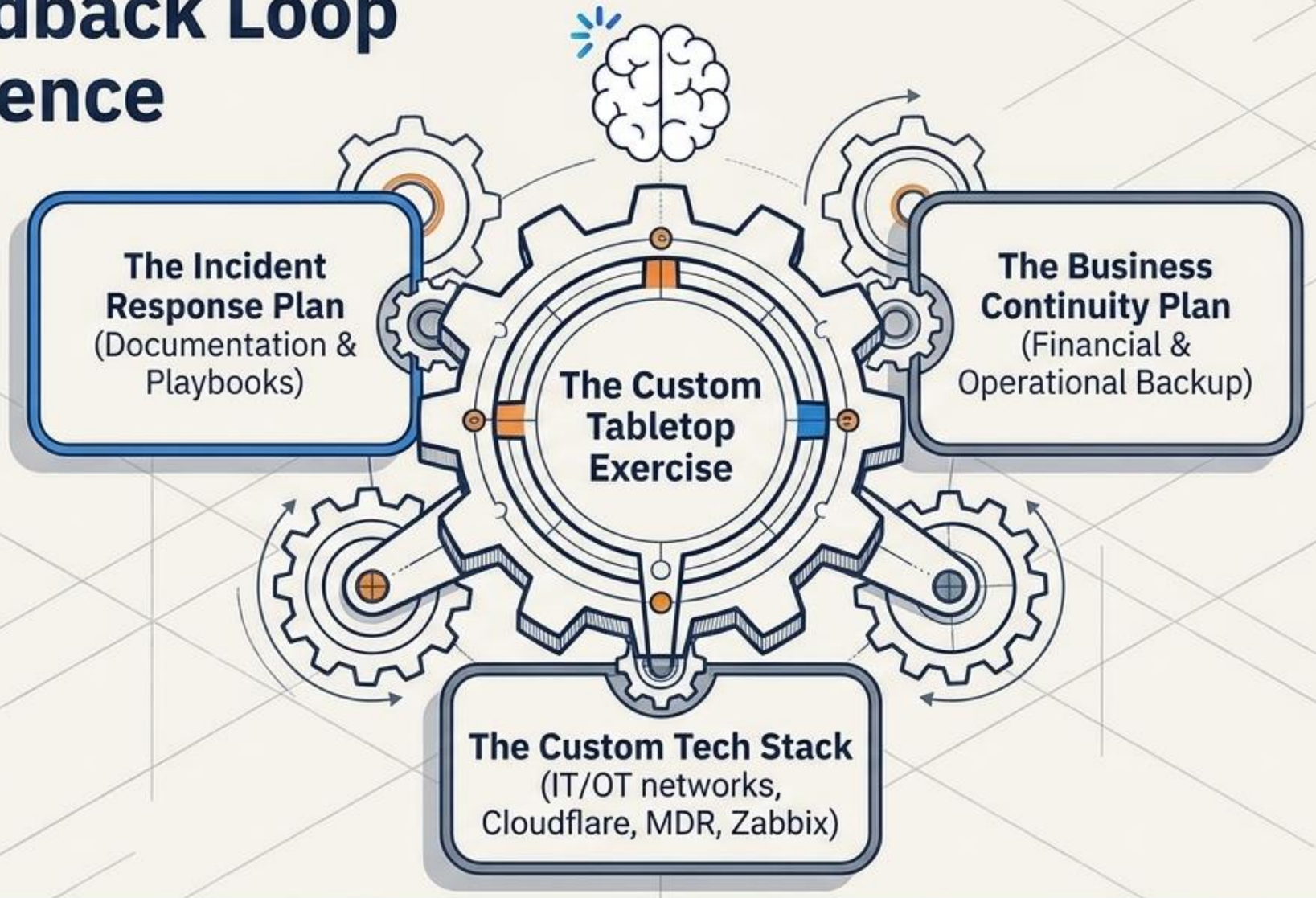
The Debrief Checklist

Honestly reflect on the incident—the good, the bad, bad, and the ugly.

Did communications flow? Were roles defined?

Update the IR plan.

The Feedback Loop of Resilience



The tabletop is the only mechanism that forces these three isolated systems to turn together under pressure.